THIS PAGE BLANK (USPTO)

(54) Title: DIGITAL WATERMARKING FOR MULTIMEDIA DATA
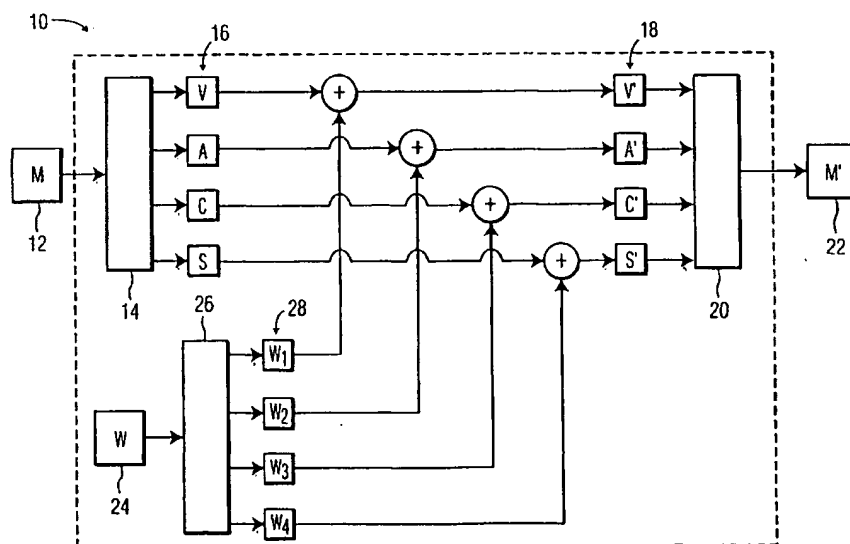
(57) Abstract: A system and method for verifying and authenticating multimedia objects. Provided is a system (26) for splitting a watermark (W) into at least a first (W1) and second part (W2), inserting the first part (W1) of the watermark (W) into a first component (V) of the multimedia object (M), and inserting the second part (W2) into a second component (A) of the multimedia object (M), and outputting (20) a watermarked multimedia object (M¹). The watermark may be provided by obtaining a signature of the original multimedia object. Also included are systems and methods for checking the validity and authenticity of a received watermarked multimedia object, wherein the multimedia object includes individual watermarked media components.

DIGITAL WATERMARKING FOR MULTIMEDIA DATA

BACKGROUND OF THE INVENTION

1. Technical Field

The present invention relates to verifying and authenticating

5   multimedia objects, and more particularly to a system and method to combine watermarks in

a plurality of multimedia components.

2. Related Art

Watermarking is the process of hiding or inserting data in multimedia

10   objects, such as audio, video and still image content. An inserted watermark can be used for

various purposes, including: (1) verification, i.e., to identify the rightful owner of the content

and protect the copyrights therein; and (2) authentication, i.e., to ensure that the content has

not been subjected to alteration.

In the case of watermarking for verification, the inserted watermark

15   can be used to identify the owner of the content. Specifically, by inserting a watermark into

the content, an owner can later prove ownership by extracting the watermark and showing

that it matches the one originally inserted. In the case of watermarking for authentication, the

inserted watermark can be used to verify the authenticity of the content by identifying content

that has been tampered with. One way to achieve this is to provide a watermark that is

20   dependent on the content. In this case, the watermark is typically a signature (or a function

of the signature) of the content. This signature is chosen so that it reflects the salient

characteristics of the content. Accordingly, if the content has been altered, the original

watermark that reflects the original signature of the content will not match the new

watermark, which reflects the signature of the tampered content.

25   Many different techniques for inserting watermarks in multimedia

components are known. A typical watermark comprises data that can identify the owner

(e.g., a visual logo) for verification; or data that captures the salient visual or auditory

characteristics of the multimedia component for content authentication. In many cases, the

watermark is inserted in the content without causing any perceivable change to the actual audio or video content. Thus, an end-user is generally not aware of the watermark.

A common problem, however, relates to ensuring that an inserted watermark has not been tampered with. For instance, consider the case of a watermarked video image. In a video image, successive frames tend to be almost identical due to the lack of motion between them. Such a lack of change between frames provides an opportunity for a hacker to identify or weaken the inserted watermark. For example, if a given frame is watermarked and the adjacent frame(s) are not watermarked, and are very similar to the watermarked frame, then the hacker can simply subtract the watermarked frame from the unwatermarked frame(s) to obtain the watermark. Identifying the watermark will enable the hacker to remove the watermark and even insert a different watermark to change the ownership rights. Even if the successive frames are watermarked (with different watermarks), the hacker can average the successive frames to weaken the watermark.

Accordingly, there exists a need to provide secure watermarking in multimedia objects, particularly those that include video. Without such a secure system, multimedia content will be subject to hackers who can easily defeat inserted watermarks.

SUMMARY OF THE INVENTION

The invention is defined by the independent claims. The dependent claims define advantageous embodiments.

This invention overcomes the above-mentioned problems, as well as others, by providing a technique to combine the watermarks in individual multimedia components, such as audio and video.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows an embodiment of a system for watermarking a multimedia object in accordance with the present invention;

Fig. 2 shows an embodiment of a watermark verification mechanism in accordance with the present invention;

Fig. 3 shows an embodiment of a watermark insertion mechanism in accordance with the present invention; and

Fig. 4 shows an embodiment of a watermark authentication system in accordance with the present invention.

5

DETAILED DESCRIPTION OF THE DRAWINGS

The present invention provides a combined watermark system and method for multimedia objects. A "multimedia object," as described herein, may comprise one or more different types of media components of unlimited type, such as audio, video, fixed images, closed caption data, compressed data, email, etc. A multimedia object may exist in any form, including a data file, data signal, data stream, data object, data structure, transmission, or program. A multimedia object may exist in a digital format or analog format.

15

Overview

For the purposes of illustration, the following overview of the invention considers a multimedia object that comprises a video component and an audio component. However, it is understood that the invention is not limited to only audio-video applications. If V represents a video frame, A represents an audio frame, and w is a watermark, then independently watermarked content $V=$ and $A=$ could be obtained as follows:

$V= = V + w$, and

$A= = A + w$.

As discussed above, such a method provides an opportunity for watermark identification and tampering, since for example, subsequent frames of a video image may be analyzed to reveal the watermark w. In the present invention, the robustness of watermark w is greatly enhanced by splitting it into two parts, w_1 and w_2. The splitting is performed by any function F such that given the two parts w_1 and w_2, the original watermark w can be uniquely and exactly computed. The splitting and inserting of the watermarks into the audio and the video frames are accomplished as follows:

$w = F(w_1, w_2),$ (1)

$V= = V + w_1$, and

$A= = A + w_2$.

Since the watermark *w* is split into two parts and inserted into the audio and video frames, a potential hacker would have to decipher both parts of the watermark. Thus, even though successive video frames are often relatively unchanged, the corresponding audio is continuously and independently varying, thereby creating a more

5   complex watermark that is much more difficult to decipher. In certain circumstances, the potential hacker would have to determine how the watermark parts w_1 and w_2 should be combined to arrive at the original watermark *w*.

As noted, the watermark *w* may be split into parts w_1 and w_2 in any manner desired (i.e., $w = F(w_1, w_2)$, where *F* could be any predetermined function.) For

10 example, the watermark may be simply separated into two smaller parts, i.e., $w = w_1 + w_2$. In such a case, since the amount of data that can be inserted into video is typically much larger than that which can be inserted into audio, the video watermark part may comprise a larger portion of the watermark data. Moreover, in order to make the system more robust, parts w_1 and w_2, could be split in a non-contiguous or non-additive manner, thereby making it more

15 difficult for a hacker to identify the original watermark *w*. For instance, the system could utilize logical operations, such as OR, AND, XOR, or various combinations of these operations, to split and combine watermarks w_1 and w_2. In order to verify the watermark, the owner could extract the two watermark parts, and combine them using the predetermined function to create the original watermark.

20 In the case of authentication watermarking, the inserted watermark is dependent on the content to be protected. To achieve this, a signature that captures the salient characteristics of the content may be extracted from the multimedia object and then inserted into the content as a signature watermark. To test the authenticity of the content, the watermark extracted from the content is compared with the signature watermark. If the

25 content is maliciously tampered, then the extracted watermark and the signature watermark would be different. As in the previous case, watermarking audio and video independently is not very robust and provides opportunities for a potential hacker to extract the watermark.

To achieve this robustness in applying an authentication watermark, combined audio-video watermarking is performed by first extracting a signature *s* that is

30 dependent on both the audio and the video components. The function *f* in the following equation extracts the salient characteristics of the audio and video. This signature is then split into two parts, as in the previous scenario and inserted into both the audio and video component.

$s = f(V, A)$,

$s = F(w_1, w_2)$,

$V = = V + w_1$, and

$A = = A + w_2$.

         In practical cases, the multimedia component might undergo some

5   processing after the watermark is inserted. Some examples of these processes include image/video/audio compression, filtering, cropping, etc. It should be recognized that the watermark insertion procedure can be implemented such that the inserted watermark w can be extracted even if the content is subjected to these alterations. However, if the alterations are so drastic that they completely alter the visual (or auditory) content of the multimedia

10   component, then it may not be possible to extract the watermark. Of course, when the multimedia component is altered so much that it does not resemble the original, the content owner may not be as concerned.

Exemplary Embodiments

15   Referring now to the figures, Figures 1-4 depict various systems for verifying and authenticating multimedia objects. The various devices, mechanisms and systems described therein may be realized in hardware, software, or a combination of hardware and software. They may be implemented by any type of computer system - or other apparatus adapted for carrying out the methods described herein. A typical

20   combination of hardware and software could be a general purpose computer system with a computer program that, when loaded and executed, controls the computer system such that it carries out the methods described herein. Alternatively, a specific use computer, containing specialized hardware for carrying out one or more of the functional tasks of the invention could be utilized. The present invention can also be embedded in a computer program

25   product, which comprises all the features enabling the implementation of the methods and functions described herein, and which - when loaded in a computer system - is able to carry out these methods and functions. Computer program, software program, program, program product, or software, in the present context mean any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing

30   capability to perform a particular function either directly or after either or both of the following: (a) conversion to another language, code or notation; and/or (b) reproduction in a different material form.

<u>1. Watermark Verification</u>

Fig. 1 depicts a system 10 for watermarking a multimedia object 12 to create a watermarked multimedia object 22. System 10 comprises a device 14 for separating the various media components 16 of multimedia object 12. Device 14 may comprise a de-

5   multiplexer or any other hardware or software system for separating the individual media components 16. Media components 16 may comprise any number of different components. Shown in Fig. 1 are a video component V, audio component A, closed caption component C and miscellaneous signal components S. Components S represent any other media component(s) that may be included in multimedia object 12.

10   Also contained in system 10 is a predefined watermark 24. A watermark generally comprises some data that can be added to the multimedia object for authentication or verification purposes. Watermark 24 may, for example, comprise the logo of a company or a certificate that has been assigned to the content owner by a central authority (this is needed to ensure that two different content owners do not use the same

15   watermark). Watermark 24 is divided into a plurality of watermark parts 28 by a splitting mechanism 26. Splitting mechanism 26 can split up the watermark 24 using any predetermined formula as previously described. For example, if the watermark contained n bits of data, a first part of the n bits could be inserted into a first watermark part w_1, the next part into w_2, the next part into w_3, and the final part into w_4. Watermark parts 28 are then

20   independently added to the media components 16 to generate a set of watermarked media components 18. Watermarked media components 18 are then combined back together by system 20 to generate a watermarked multimedia object 22. Device 20 may comprise a multiplexer or any other hardware or software system for combining the media components into watermarked multimedia object 22. The resulting watermarked multimedia object 22

25   contains independently watermarked media components.

Referring now to Fig. 2, a verification mechanism 11 is shown that can verify the watermark in the watermarked multimedia object 22 created by the system of Fig. 1. Verification mechanism 11 first divides watermarked multimedia object 22 into a set of watermarked media components 19 using device 30. Similar to device 14 shown in Fig. 1,

30   device 30 may comprise a de-multiplexer or any other hardware or software system for breaking the watermarked multimedia object 22 into individual watermarked media components 19. The watermarked media components 19 are then inputted into a watermark extraction mechanism 32 that extracts the watermarked parts 34 from each of the watermarked media components 19. Watermarked parts 34 are then combined together using

combining mechanism 36 to generate an extracted watermark 38. Combining mechanism 36 combines the watermark parts 34 based on the same formula that splitting mechanism 26 shown in Fig. 1 used to split the original watermark. The extracted watermark 38 is then compared with the original watermark 24 by comparator 40. The results of the compare operation are then generated as output 42. If the watermarks match within a certain threshold, then it establishes that the multimedia component belongs to the content owner whose watermark appeared in the content.

2. Multimedia Object Authentication

Referring now to Fig. 3, a watermark insertion system 45 used for authenticating purposes is shown, which converts multimedia object 44 into a watermarked multimedia object 60. Similar to the embodiment depicted in Fig. 1, system 45 includes a device 46 for extracting the individual media components 48 that make up multimedia object 44. Device 46 further includes a mechanism for extracting a signature 50 of the multimedia object 44. While device 46 is shown in a single functional block, it understood that the system for extracting a signature may be functionally separated from the system that extracts the media components 48. Signature 50 contains data that is representative of the data contained in multimedia object 44. Many different ways of extracting the signature are known in the art. In this embodiment, the signature 50 is used as the watermark W. As an alternative, watermark W could be a function of the signature 50.

In a manner similar to the embodiment depicted in Fig. 1, the watermark is then split into a set of watermarked parts 54 by a splitting mechanism 52. Any predetermined formula for splitting the watermark W can be used. The individual watermarked parts 54 are then added to the media components 48 to provide a set of watermarked media components 56. The watermarked media components 56 are then combined using combining mechanism 58 to generate a watermarked multimedia object 60.

Referring now to Fig. 4, an authentication system 61 is depicted for authenticating a watermarked multimedia object 60 that includes independently watermarked media components, such as that created by system 45 shown in Fig. 3. System 61 includes a first device 62 for extracting each of the watermarked media components 64. A second device 66 is provided for extracting the watermarked parts 68 from each of the watermarked media components 64. In addition, device 66 extracts the signature of the received multimedia object, which acts as a signature watermark 74. It should be recognized that a separate device could be used to extract the signature of the watermarked multimedia object

60. Signature watermark 74 is extracted using the same formula that was used to create the
original watermark inserted into multimedia object 60, as shown in Fig. 3.

The extracted watermark parts 68 are then combined with combining
mechanism 70 to generate an extracted watermark 72. Combining mechanism 70 combines

5   the watermark components 68 using the same ratio, formula or system as splitting mechanism
52, shown in Fig. 3, used to split them. The extracted watermark 72 is then compared with
the signature watermark 74 using comparing mechanism 78. The result of the compare is
then generated as output 80. If the two watermarks match within a degree of threshold, then
the multimedia object 60 is authenticated. Conversely if the two watermarks 72 and 76 do

10   not match, then it is known that the watermarked multimedia object 60 is no longer authentic.

The foregoing description of the preferred embodiments of the
invention have been presented for purposes of illustration and description. They are not
intended to be exhaustive or to limit the invention to the precise form disclosed, and
obviously many modifications and variations are possible in light of the above teachings.

15   Such modifications and variations that are apparent to a person skilled in the art are intended
to be included within the scope of this invention as defined by the accompanying claims. In
the claims, any reference signs placed between parentheses shall not be construed as limiting
the claim. The word "comprising" does not exclude the presence of elements or steps other
than those listed in a claim. The word "a" or "an" preceding an element does not exclude the

20   presence of a plurality of such elements. The invention can be implemented by means of
hardware comprising several distinct elements, and by means of a suitably programmed
computer. In the claim enumerating several means, several of these means can be embodied
by one and the same item of hardware. The mere fact that certain measures are recited in
mutually different dependent claims does not indicate that a combination of these measures

25   cannot be used to advantage.

CLAIMS:

1.   A method of protecting a multimedia object having a first media component and a second media component, comprising the steps of:

providing a watermark;

splitting the watermark into a first part and a second part;

inserting the first part of the watermark into the first media component;

inserting the second part of the watermark into the second media component; and

outputting a watermarked multimedia object.

2.   The method of claim 1, comprising the further steps of:

receiving the watermarked multimedia object;

extracting from the first media component of the watermarked multimedia object a first extracted watermark part;

extracting from the second media component of the watermarked multimedia object a second extracted watermark part;

combining the first extracted watermark part with the second extracted watermark part; and

comparing the combined first and second extracted watermark parts with the provided watermark to verify an ownership.

3.   The method of claim 1, wherein the watermark is a signature watermark and is provided by:

obtaining a signature of the multimedia object; and

generating the signature watermark as a function of the signature.

4.   The method of claim 3, comprising the further steps of:

receiving the watermarked multimedia object;

extracting from the first media component of the watermarked multimedia object a first extracted watermark part;

extracting from the second media component of the watermarked multimedia object a second extracted watermark part;

generating a combination watermark by combining the first extracted watermark part with the second extracted watermark part;

5   generating a signature watermark that is a function of a signature extracted from the watermarked multimedia object; and

comparing the combination watermark with the signature watermark to authenticate the multimedia object.

10   5.   A system for protecting a multimedia object having a first media component and a second media component, comprising:

a mechanism (26) for splitting a watermark into a first and a second part; and

a mechanism for inserting the first part into the first media component, and for inserting the second part into the second media component.

15

6.   The system of claim 5, further comprising a mechanism (20) for outputting a watermarked multimedia object, wherein the watermarked multimedia object includes the first media component having the first part of the watermark, and the second media component having the second part of the watermark.

20

7.   The system of claim 5, wherein the first media component is an audio component, and the second media object is a video component.

8.   The system of claim 6, further comprising:

25   a mechanism (46) for obtaining a signature from the multimedia object; and

a mechanism (46) for generating the watermark as a function of the signature.

9.   The system of claim 6, further comprising:

a mechanism (32) for extracting a first extracted watermark part from the first

30   media component in the watermarked multimedia object, and for extracting a second extracted watermark part from the second media component in the watermarked multimedia object;

a mechanism (36) for combining the first extracted watermark part with the second extracted watermark part; and

a mechanism (40) for comparing the combined first and second extracted watermark parts with the watermark.

10.   The system of claim 8, further comprising:

a mechanism (66) for extracting a first extracted watermark part from the first media component in the watermarked multimedia object, and for extracting a second extracted watermark part from the second media component in the watermarked multimedia object;

a mechanism (70) for generating an extracted watermark by combining the first extracted watermark part with the second extracted watermark part;

a mechanism (66) for generating a signature watermark that is a function of a signature of the watermarked multimedia object; and

a mechanism (78) for comparing the extracted watermark with the signature watermark.

11.   A system for authenticating a watermarked multimedia object having a first media component and a second media component, comprising:

a mechanism (32) for extracting a first watermark part from the first media component, and for extracting a second watermark part from the second media component;

a mechanism (36) for combining the first extracted watermark part with the second extracted watermark part; and

a mechanism (40) for comparing the combined first and second watermark parts with a provided watermark.

12.   The system of claim 11, wherein the provided watermark is generated as a function of a signature of the watermarked multimedia object.

13.   The system of claim 11, wherein the first media component is a video component and the second media component is an audio component.

14.   The system of claim 13, wherein the watermarked multimedia object has a third media object, and wherein the third media object is a closed caption component.
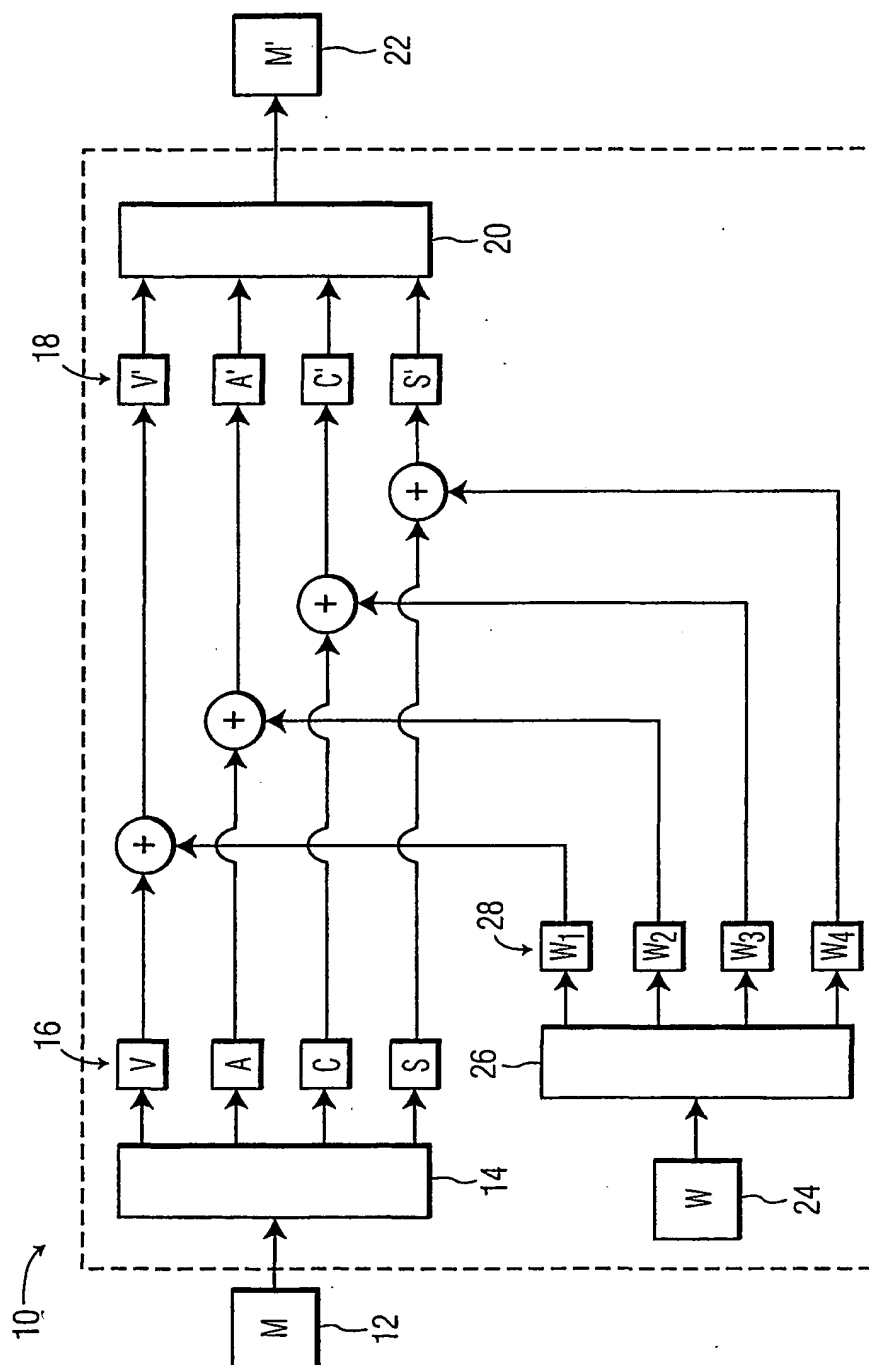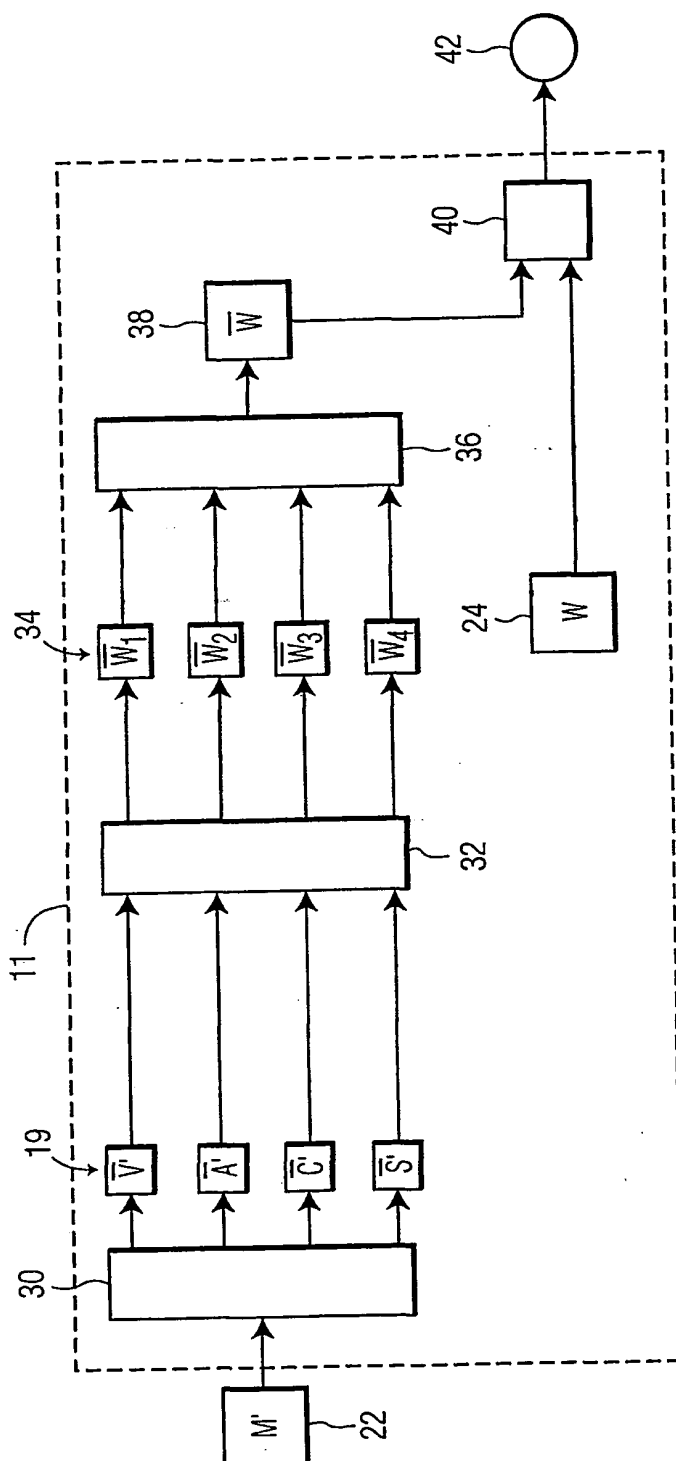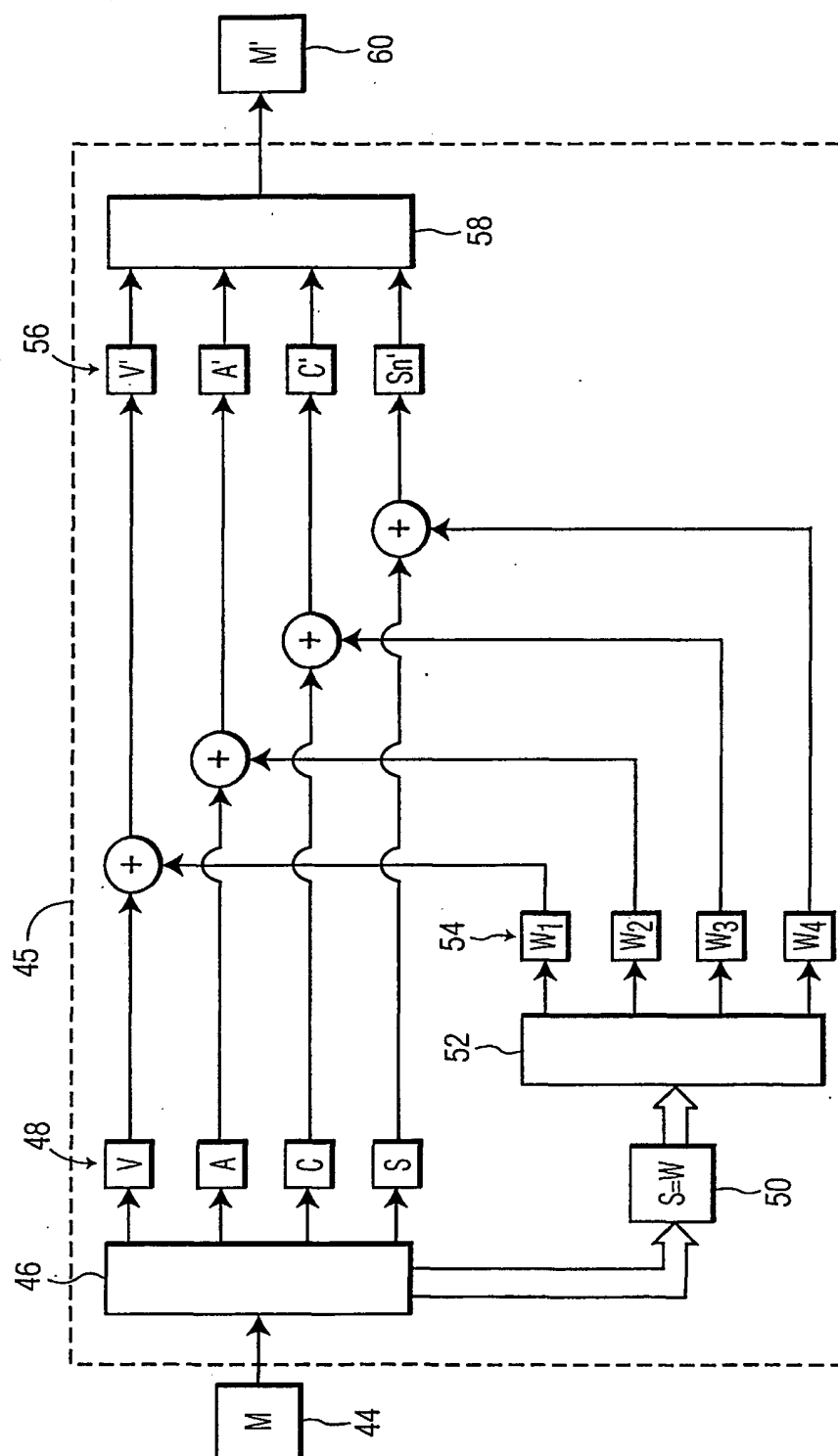
1/4

FIG. 1

FIG. 2

FIG. 3

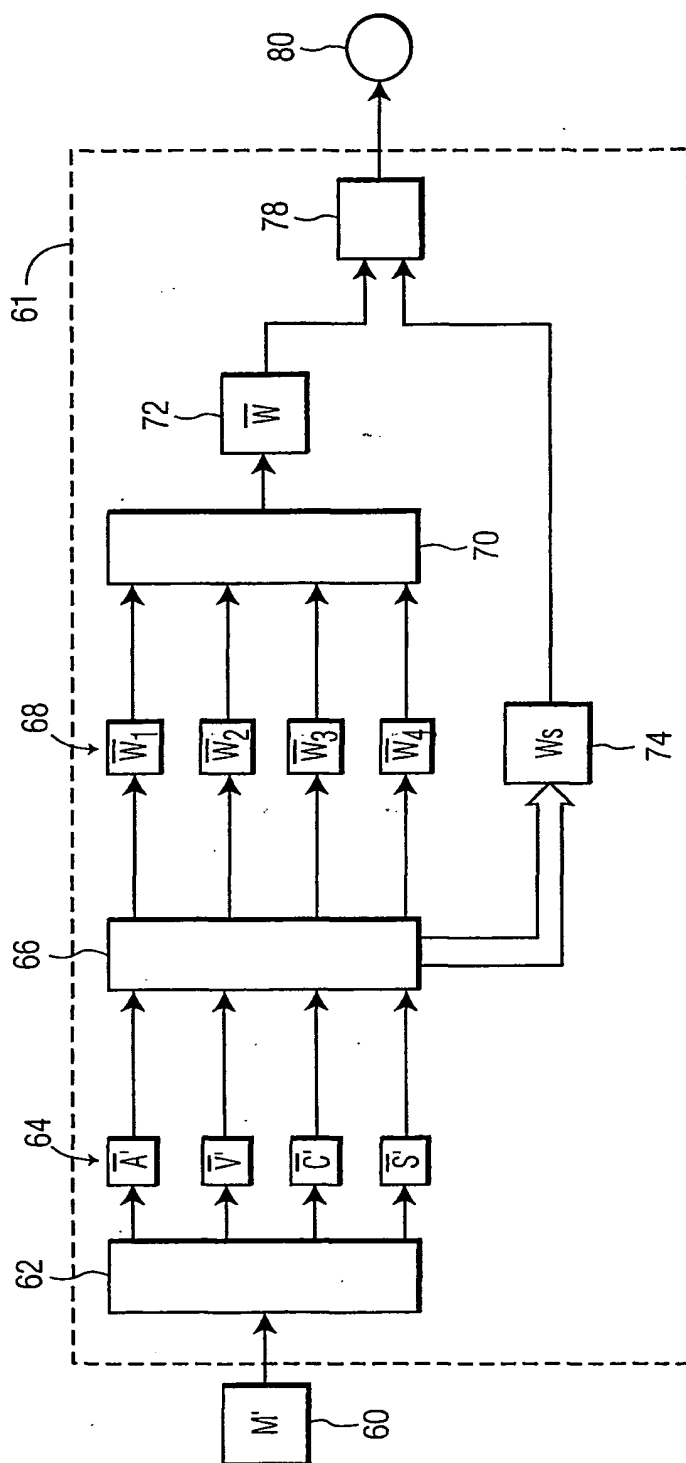FIG. 4

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04N5/913   G06T1/00   H04N7/52

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   H04N   G06T

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category°	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DITTMANN J ET AL: "COMBINED VIDEO AND AUDIO WATERMARKING: EMBEDDING CONTENT INFORMATION IN MULTIMEDIA DATA" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 3971, 2000, pages 455-464, XP000980610 the whole document --- -/--	1-14

| X | Further documents are listed in the continuation of box C. | X | Patent family members are listed in annex. |

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 December 2001	28/12/2001

| Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,
Fax: (+31–70) 340–3016 | Authorized officer

Gries, T |

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DITTMANN J ET AL: "MEDIA-INDEPENDENT WATERMARKING CLASSIFICATION AND THE NEED FOR COMBINING DIGITAL VIDEO AND AUDIO WATERMARKING FOR MEDIA AUTHENTICATION" PROCEEDINGS INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: CODING AND COMPUTING, XX, XX, 27 March 2000 (2000-03-27), pages 62-67, XP000992579 the whole document	1-14
A	EP 0 843 471 A (SONY CORP) 20 May 1998 (1998-05-20) abstract; claims	1-14
A	EP 0 855 837 A (SONY CORP) 29 July 1998 (1998-07-29) abstract; claims	1-14
A	EP 0 952 728 A (IBM) 27 October 1999 (1999-10-27) abstract; claims; figures	1-14

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0843471	A	20-05-1998	JP	10149621 A	02-06-1998
			EP	0843471 A1	20-05-1998
			US	6112008 A	29-08-2000
EP 0855837	A	29-07-1998	JP	10210436 A	07-08-1998
			CA	2227380 A1	23-07-1998
			EP	0855837 A2	29-07-1998
			TW	388181 B	21-04-2000
			US	2001010756 A1	02-08-2001
			US	2001046101 A1	29-11-2001
EP 0952728	A	27-10-1999	US	6256736 B1	03-07-2001
			EP	0952728 A2	27-10-1999
			JP	2000083159 A	21-03-2000